様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １４ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2015～2017
課題番号：１５Ｈ０２６８７

研究課題名（和文）安全な協調ロボット制御ソフトウェア開発方法の研究

研究課題名（英文）A Development Process of Control Software for Safe Cooperative Robots

研究代表者
磯部　祥尚（Isobe, Yoshinao）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：５０３５６４５８

交付決定額（研究期間全体）：（直接経費）　　12,900,000円

研究成果の概要（和文）：自律・分散・協調ロボットの制御ソフトウェアの安全性向上を目的として、制御の振舞いを厳密に記述・検証するために形式手法を適用した。その成果は、定理証明器による運動制御の形式検証技術とモデル検査器による協調制御の形式検証技術から成る。運動制御では、ロボットの運動学（キネマティクス）のライブラリを定理証明器Coq上に形式化し、その有効性をロボットアームの形式化・検証に適用して実証した。協調制御では、協調搬送ロボットを例に、設計（有限状態機械）、形式化（仕様記述言語CSP）、検証（モデル検査器FDR）、実装（ミドルウェアRTM）の各工程を連携させ、設計段階で協調動作の不具合を検出できることを示した。

研究成果の学術的意義や社会的意義
大規模IoT化が進むなか、大量のモノが高速で連携する自律・分散・協調システムの重要性が高まりつつある。その一方で、協調動作では発生確率の低いタイミング依存の不具合が潜在化する可能性があり、実装後のテストでは検出しきれないなどの問題がある。本研究では、運動制御と協調制御の形式記述と検証の作業コスト削減可能なライブラリを作成し、ロボットアームと協調搬送ロボットを例として、形式化の効果を示した。産業界への形式手法導入は容易ではないが、本研究のように、その効果と作業コスト削減の可能性を示すことによって、形式手法は今後の自律・分散・協調システムの安全性向上に資する技術となりうる。

研究成果の概要（英文）：In order to improve the safeness of autonomous distributed cooperative robots, we applied formal methods for logically describing and verifying their control software in this research. The research result consists of the formal verification techniques for motion control by a theorem prover and for cooperative control by a model checker. For the verification of motion control, we developed a formal library about robot motion (kinematics) in the theorem prover Coq, and demonstrated its usefulness by formalizing and verifying the SCARA robot manipulator. For the verification of cooperative control, we showed how to detect design errors before the implementation by seamlessly connecting design (as finite state machines), formalization (in the specification and description language CSP), verification (by the model checker FDR), and implementation (by the middleware RTM) phases.

研究分野：形式手法

キーワード：協調ロボット　制御ソフトウェア　安全性　形式手法　検証　モデル検査　定理証明　有限状態機械

１．研究開始当初の背景

近年、ロボット技術の進歩とともに、工場のような閉鎖された場所だけでなく、人間と協働するロボットや、他のロボットと協調するロボットのように、協調型のロボットが登場してきている。しかし、協調動作の相互作用を適切に把握し、設計することは難しく、人間に危害を加えるような誤動作が混入する可能性もある。協調ロボットを安心して利用できるように、その安全性と信頼性の向上が課題となっている。

２．研究の目的

本研究では、図 1 のような、自律・分散・協調するロボットの制御ソフトウェアの安全性と高信性の向上を目的として、制御ソフトウェアを設計・検証・実装するための開発方法の確立を目標とする。図 1 の運動制御部は目標位置までの速度（振舞い）の設定等、連続的な制御を担当し、協調制御部は他の協調制御部と相互にデータを送受信しながら、目標位置（動作モード）の変更等、離散的な制御を担当する。

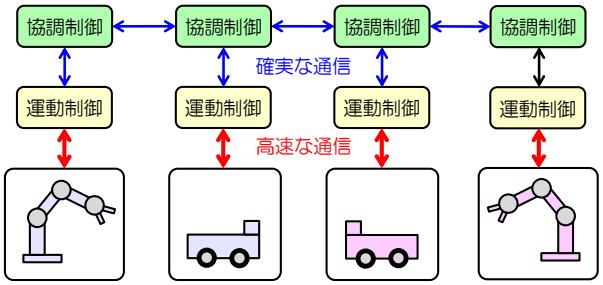

図 1　自律・分散・協調ロボット

３．研究の方法

安全で高信頼な協調ロボット制御ソフトウェアの開発を支援するため、図 1 に示す協調制御部と運動制御部を適切に設計・検証・実装する技術を研究開発する。

ロボットソフトウェアの実装には、協調するロボットの機能要素（**RTC**：Robotic Technology Component）間の連携を可能にするロボット用プラットフォーム（**RTM**：RT Middleware）を利用する。RTM では、有限状態機械（**FSM**：Finite State Machine）をもつ RTC を実装するためのライブラリ **FSM4RTC** の開発が進められており、複数の動作モード（接近、待機、搬送、充電など）をもつ制御ロジックの実装に適している。

有限状態機械で表現される RTC の形式化（モデル化）には **CSP**（Communicating Sequential Processes）を利用する。CSP は協調する有限状態機械を形式的に（厳密に）記述・解析可能な仕様記述言語である。CSP で形式的に記述された協調有限状態機械の振舞いを網羅的に自動的に検証するためには、モデル検査器 **FDR** を利用する。FDR は CSP の代表的な検証ツールである。

一方、CSP は協調する離散的な振舞いの形式化には適しているが、連続的な振舞いの形式化には適していない。そこで、運動制御部の形式化には強力な証明能力をもつ定理証明器 **Coq** を利用する。Coq の証明は半自動であるが、複雑な運動制御の表現が可能である。

なお、協調制御部の設計、検証、実装については、当初の計画では、設計から実装までをシームレスにつなぐために CSP 方式（検証に適する同期通信方式）を共通仕様としていたが、同期待ちする CSP 方式では実行効率に問題があると判断し、同期待ちをしない FSM4RTC 方式（実装に適する非同期通信方式）を共通仕様とするように計画を変更した。

４．研究成果

(1) 運動制御の形式化

ロボットアームを主な対象として、運動制御の静的な性質と動的な性質の形式化を行い、ロボットアームの振舞いを形式的に（厳密に）解析するためのライブラリを構築した。そのライブラリをロボットアームの形式化に適用し、その記述・検証能力を実証した。以下、静的/動的な性質の形式化について説明する。

① 位置と角度の形式化（静的）：運動制御の最初の形式化として、キネマティクス（ロボットの運動学）の基礎となる性質を定理証明器 Coq 上に形式化した。具体的には、キネマティクスの基礎となる座標、回転、剛体力学の基本的性質と、剛体変換の様々な表現（等長写像、同次表現、Denavit-Hartenberg 変換、らせん運動）を定理証明器 Coq 上に形式化した。形式化した剛体変換によるロボットマニピュレータの形式化への適用事例として、図 2 の SCARA 型ロボットアー

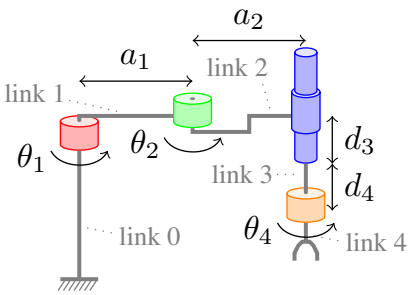

図 2　SCARA 型ロボットアームのモデル

ムの振舞いを Coq 上に形式化した。このキネマティクスの形式化によって、ロボットアームの各関節の角度と腕の長さから手先の位置の形式的推論が可能になった。その成果を形式検証の国際会議（〔学会発表〕⑤）で発表するとともに、その解析論文を学術論文誌（〔雑誌論文〕①）にて発表した。

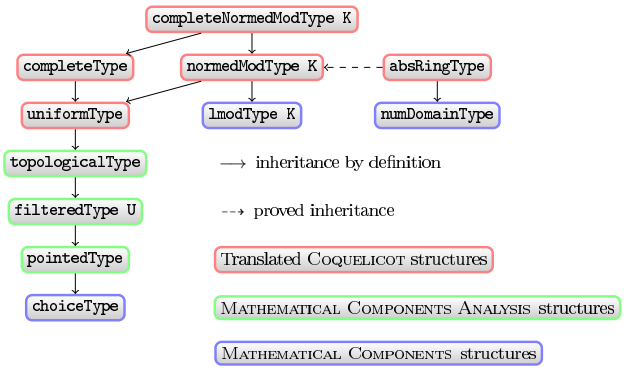

図 3　拡張された Coq ライブラリ階層構造

② 速度の形式化（動的）：ロボットアームの動き（各関節の速度と手先の速度の関係）を表現するために、前述の静的な性質の形式化を基盤にして、ヤコビ行列を形式化した。さらに、SCARA 型ロボットアームの動きをヤコビ行列によって Coq 上に形式化し、その証明スクリプト（Coq コード）をウェブサイト GitHub から公開した（〔その他〕①②）。また、ヤコビ行列の形式化に必要な数学（微分等）をライブラリ MathComp-Analysis として形式化し（図 3 参照）、国際学会（〔学会発表〕①）で発表するとともに、形式的な実数解析のための基本技術をまとめた論文を学術雑誌（〔雑誌論文〕①）に発表した。

(2) 協調制御の形式化

協調ロボットの設計から検証・実装までをシームレスに行う方法を考案し、その方法を協調搬送ロボット TransRobo の開発事例に適用して有効性を示した。その成果をロボットの講演会（〔学会発表〕②③）で発表した。以下、作成した設計と実装について、その検証と修正とともに説明する。

① 協調制御の設計：協調搬送ロボット TransRobo の RTC（RT コンポーネント）の接続図、協調制御部 RoboMng の有限状態機械、運動制御部 RoboCtrl の有限状態機械を、各々図 4、図 5、図 6 に示す。協調制御部は 4 つのモード（充電、接近、待機、搬送）をもち、自機の運動制御部からのイベント（目的地到着等）や他機の協調制御部からのイベント（準備完了、取消）に応じて、自機のモード変更や他機へのイベント送信を行う。運動制御部 RoboCtrl は協調制御部からの指示に従い、ロボット本体に移動速度を送信する。なお、ここでは、協調動作の検証を目標にしているため、移動経路や速度などの具体的な値は抽象化し、イベントの送受信の実行順序を検証の対象にしている。また、後で検証の効果を説明するため、図 5 には完成版のひとつ前の（ミスがある）版を掲載している。

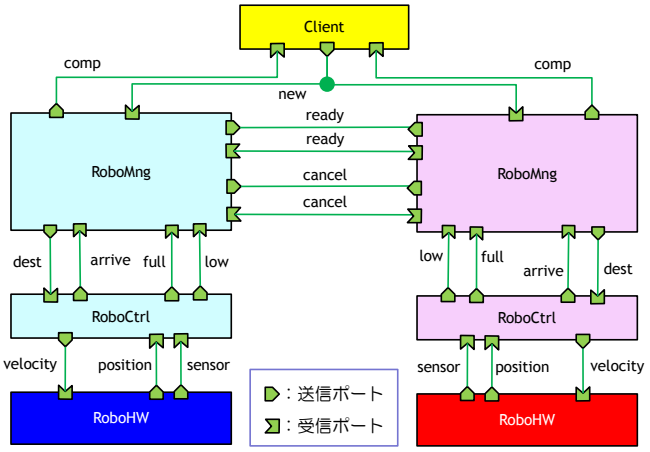

図 4　TransRobo の RTC の接続図

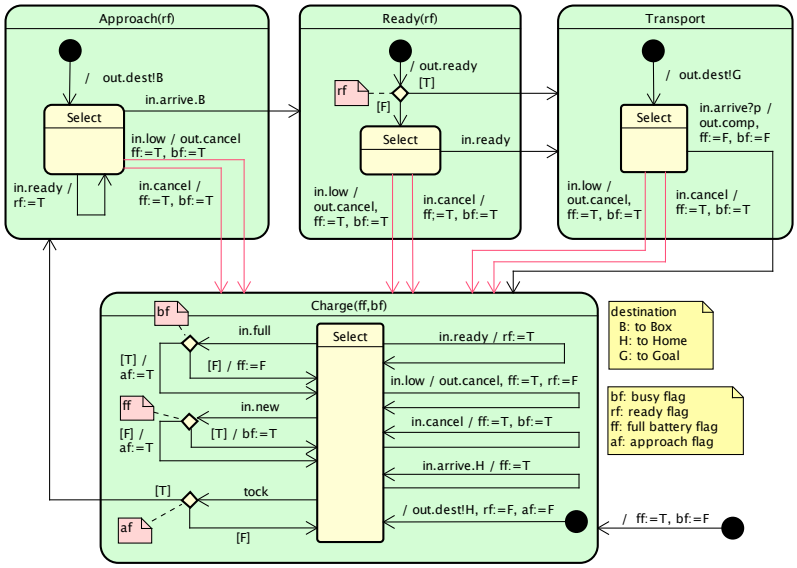

図 5　協調制御部 RoboMng の有限状態機械

② 協調制御の設計の形式化と検証：図 5 に示すように、個々の有限状態の振舞いは簡潔でも、複数の有限状態機械が協調することによって、その全体の振舞いは複雑になり、正確に把握することは困難になる。そこで、本研究では、接続関係と個々の有限状態機械を形式仕様記述言語 CSP で形式化し、モデル検査器 FDR で網羅的に検証した。

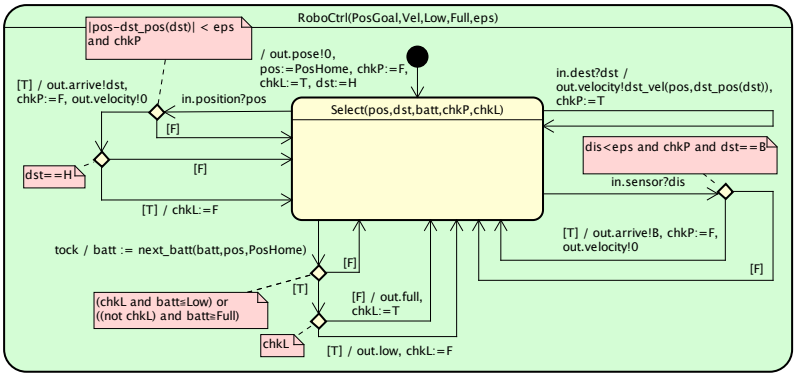

図 6　運動制御部 RoboCtrl の有限状態機械

本研究では、FSM4RTC 方式の協調ロボットの設計を簡単に記述・検証できるように、FSM4RTC 準拠の検証ライブラリをモデル検査器 FDR 用に作成した。このライブラリによって、協調搬送ロボット TransRobo の形式化と検証にかかる作業のコストや形式化のミスを削減することができた。図 7 に TransRobo の設計（図 4、図 5、図 6）を CSP で形式化し、FDR で検証した結果を示す。図 7 右側の 6 項目が検証結果を表しており、検証した性質は上から順に、(ⅰ)デッドロックしない、(ⅱ)ライブロックしない、(ⅲ)有限時間内に無限のイベントを実行しない、(ⅳ)期待する正常動作を含む、(ⅴ)単独搬送しない、(ⅵ)送信はブロックされない、である。

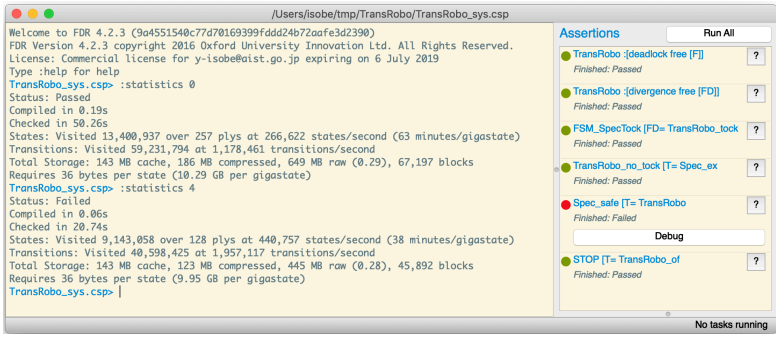

図 7　協調搬送ロボット TransRobo の設計（CSP）の検証結果

③ 協調制御の設計の修正：図 7 では、5 番目の性質「単独搬送しない」の検査結果が failed になっており、これは搬送ロボットが単独搬送する可能性があることを示している。モデル検査器では、性質が成り立たない状態がある場合は、その状態に至る例（反例）を表示できる。図 8 に、単独搬送に至る反例の FDR による表示画面と、その反例を解析した結果を示す。この解析結果は、Robo1 の ready イベントの送信と、Robo2 の cancel イベントの送信がほぼ同時に発生したときに、Robo2 が受信した ready イベントが取り消されずに、単独搬送に至る可能性があることを表している。この単独搬送が発生する確率は非常に低いが 0 ではない。このようなタイミング依存の不具合をテストで発見することは困難であり、この例は網羅的なモデル検査の有効性を示している。図 8 の解析結果に示すように、この単独搬送の誤動作は、待機状態で cancel イベントを受信した場合、その直後に cancel イベントを返送するように修正することによって解消できると考えられる。実際には、待機状態と搬送状態にそのような返送を追加することによって単独搬送の誤動作が解消されることを FDR で確認した。なお、同様に充電状態で cancel イベントを受信後にも cancel イベントの返送を追加すると、cancel イベントが無限に送受信されるライブロックが発生する。協調制御の設計には細心の注意が必要である。

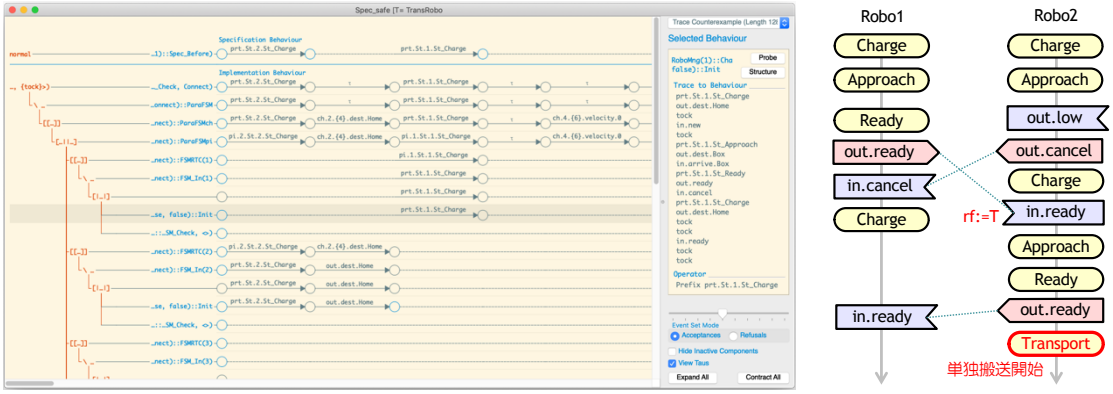

図 8　協調搬送ロボットが単独搬送に至る反例表示（左）とその解析結果（右）

④ 協調制御の実装：前述の協調搬送ロボットの設計、形式化、検証、修正を繰り返し行い、6 個全ての検証項目が passed になることを確認後、協調制御部 RoboMng の RTC を FSM4RTC ライブラリで実装した。また、運動制御部 RoboCtrl の RTC は、搬送ロボットのハードウェア（図 4 の RoboHW）として Raspberry Pi Mouse（RTC 対応）を想定して実装した。これらの RTC を作成後、RT system editor で RTC を接続し、RTM 上で協調搬送ロボットの制御を実行した例を図 9 に示す。図 9 左は system editor による接続画面、中央は 2 台の搬送ロボットの協調動作を確認するための簡易シミュレータ、右は Raspberry Pi Mouse の振舞いを確認するためのシミュレータの画面である。現在、2 台の Raspberry Pi Mouse の実機を用いた協調搬送の実証実験の準備を進めている。今後も本研究の情報をウェブサイト（〔その他〕③）から発信していく。

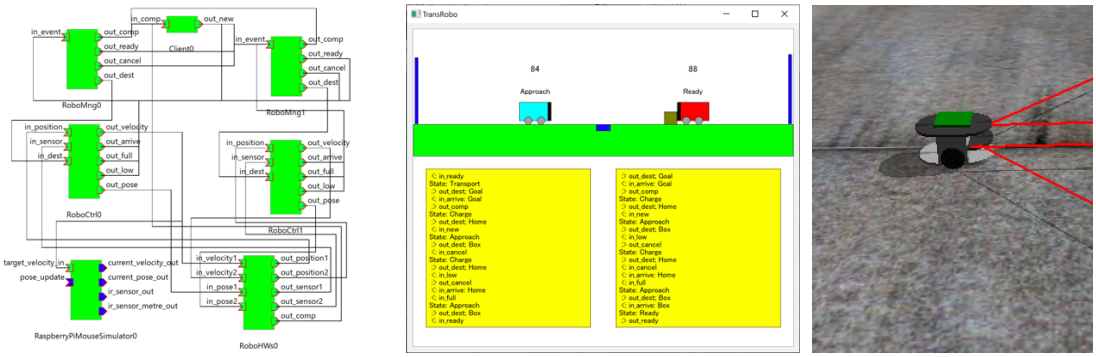

図 9　RT system editor による RTC の接続（左）とその実行例（中、右）

５．主な発表論文等

〔雑誌論文〕（計 2 件）

① Reynald Affeldt, Cyril Cohen, and Damien Rouhling, Formalization Techniques for Asymptotic Reasoning in Classical Analysis, Journal of Formalized Reasoning, Vol.11, No.1, pp.43-76, 2018.（査読有）DOI: 10.6092/issn.1972-5787/8124
② アフェルト レナルド, Mathematical Components 入門, コンピュータソフトウェア, vol.34, pp.34-74, 2017.（査読有）DOI: https://doi.org/10.11309/jssst.34.2_64

〔学会発表〕（計 8 件）

① Reynald Affeldt, Cyril Cohen, Assia Mahboubi, Damien Rouhling, and Pierre-Yves Strub Classical analysis with Coq, The Coq Workshop 2018, Oxford, UK, July 8, 2018.
② 磯部 祥尚, 安藤 慶昭, 宮本 信彦, ビグズ ジェフ, 大岩 寛,協調ロボット制御ロジックの形式的なモデル化と検証 - FSM4RTC のための有限状態マシン設計の信頼性向上 -, ロボティクス・メカトロニクス講演会 ROBOMECH2018, pp.2A1-F11, 2018.
③ 安藤 慶昭, 宮本 信彦, 高橋 三郎, ビグズ ジェフ, 花井 亮, 原 功, FSM コンポーネント実装フレームワークの提案 - FSM4RTC 標準に準拠した状態遷移型コンポーネント実装 -, ロボティクス・メカトロニクス講演会 ROBOMECH2017, pp.2A2-J10, 2017.
④ 磯部 祥尚, 協調ロボット制御ロジックの設計モデル検証, 第 21 回 CSP 研究会, 2018.
⑤ Reynald Affeldt and Cyril Cohen, Formal Foundations of 3D Geometry to Model Robot Manipulators, CPP 2017 - Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs, pp.30-42, 2017（国際学会）.
⑥ Reynald Affeldt and Cyril Cohen, Formal Foundations for Rigid Body Transformation, 日本ソフトウェア科学会第 33 回大会, 2016.
⑦ 磯部 祥尚, 協調制御のモデル化と解析に向けて, 第 17 回 CSP 研究会, 2016.
⑧ 安藤 慶昭, 状態遷移コンポーネントとデータポートに関する標準 FSM4RTC について, 第 17 回計測自動制御学会 システムインテグレーション部門講演会, 2016

〔その他〕
ホームページ等

① Formal Foundations of 3D Geometry to Model Robot Manipulators
https://staff.aist.go.jp/reynald.affeldt/robot/
② Formal Foundations for Modeling Robot Manipulators
https://github.com/affeldt-aist/coq-robot
③ 協調ロボット制御ロジックの形式的なモデル化と検証
https://staff.aist.go.jp/y-isobe/coop-robo/

６．研究組織

(1)研究分担者
研究分担者氏名：大岩 寛 （OIWA, Yutaka）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：研究チーム長
研究者番号（8桁）：20415649

(2)研究分担者
研究分担者氏名：アフェルト レナルド （AFFELDT, Reynald）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：主任研究員
研究者番号（8桁）：40415641

(3)研究分担者
研究分担者氏名：安藤 慶昭 （ANDO, Noriaki）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：研究チーム長
研究者番号（8桁）：50371018

(4)研究分担者
研究分担者氏名：ビグズ ジェフ （BIGGS, Geoffrey）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：主任研究員
研究者番号（8桁）：20534803

(5)研究分担者
研究分担者氏名：花井 亮 （HANAI, Ryo）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：研究員
研究者番号（8桁）：10521255

(6)研究分担者
研究分担者氏名：中坊 嘉宏 （NAKABO, Yoshihiro）
所属研究機関名：国立研究開発法人産業技術総合研究所
部局名：情報・人間工学領域
職名：研究チーム長
研究者番号（8桁）：70360609